Common Criteria

ACO Composition in v3.0

David Martin CESG UK

Common Criteria

History of inclusion

- CCv2.x traditionally applied to component TOEs
- What happens when putting together the results of individual component TOEs?

  = results of two individual component TOEs
- Further analysis is required to determine assurance of the composed TOE

Common Criteria

Types of composition

- Layered
  - On same platform
  - Base provides services to dependent
- Examples
  - Database is dependent component on an operating system base component
  - Money purse application is dependent component on a smart card base component

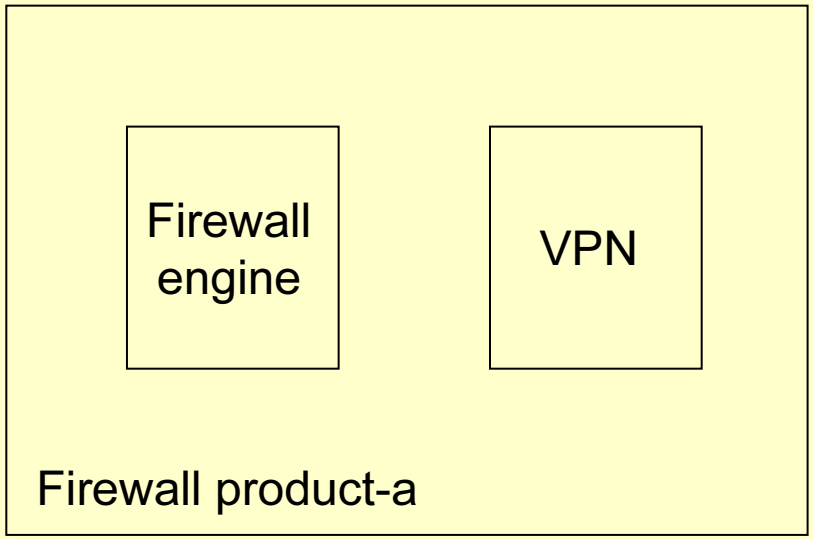
Common Criteria

Types of composition

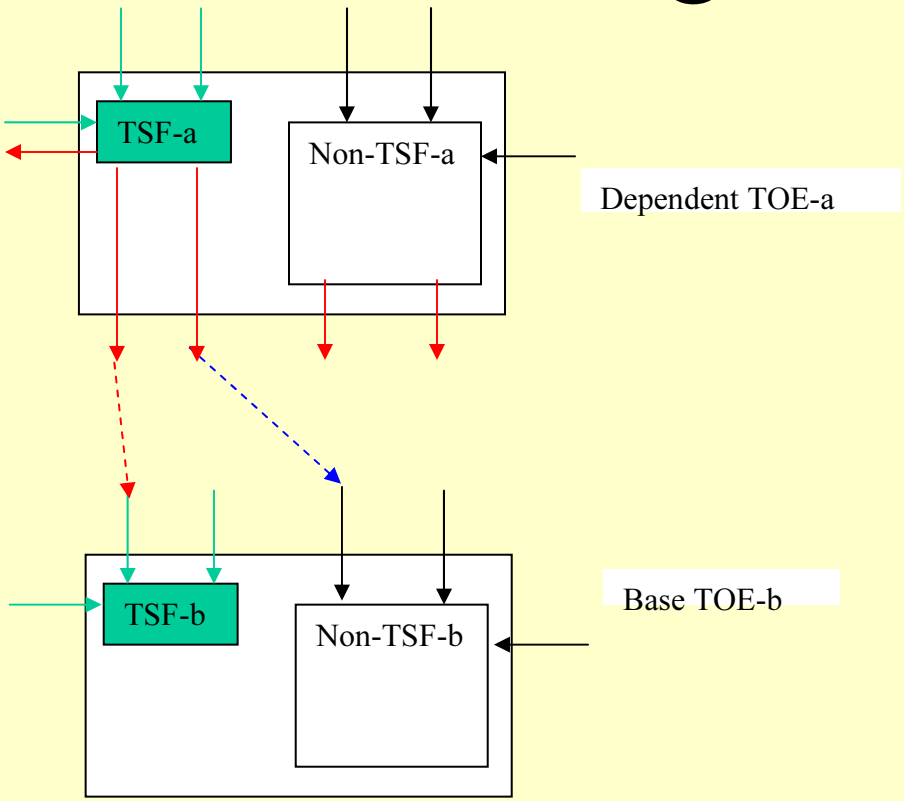
- Peer-to-peer
  - Peers are dependent on each other
  - Mutual dependency can be dealt with through iteration of reliance analysis
  - Reliance becomes blurred when peer-to-peer TOEs are located on the same platform
  - Need to designate one as base:
    - Authentication server is base component for an operating system
    - Audit log server is base component for a firewall appliance

Common Criteria

Composition stumbling blocks



Composition Stumbling Blocks



Design information required for new TSF portion

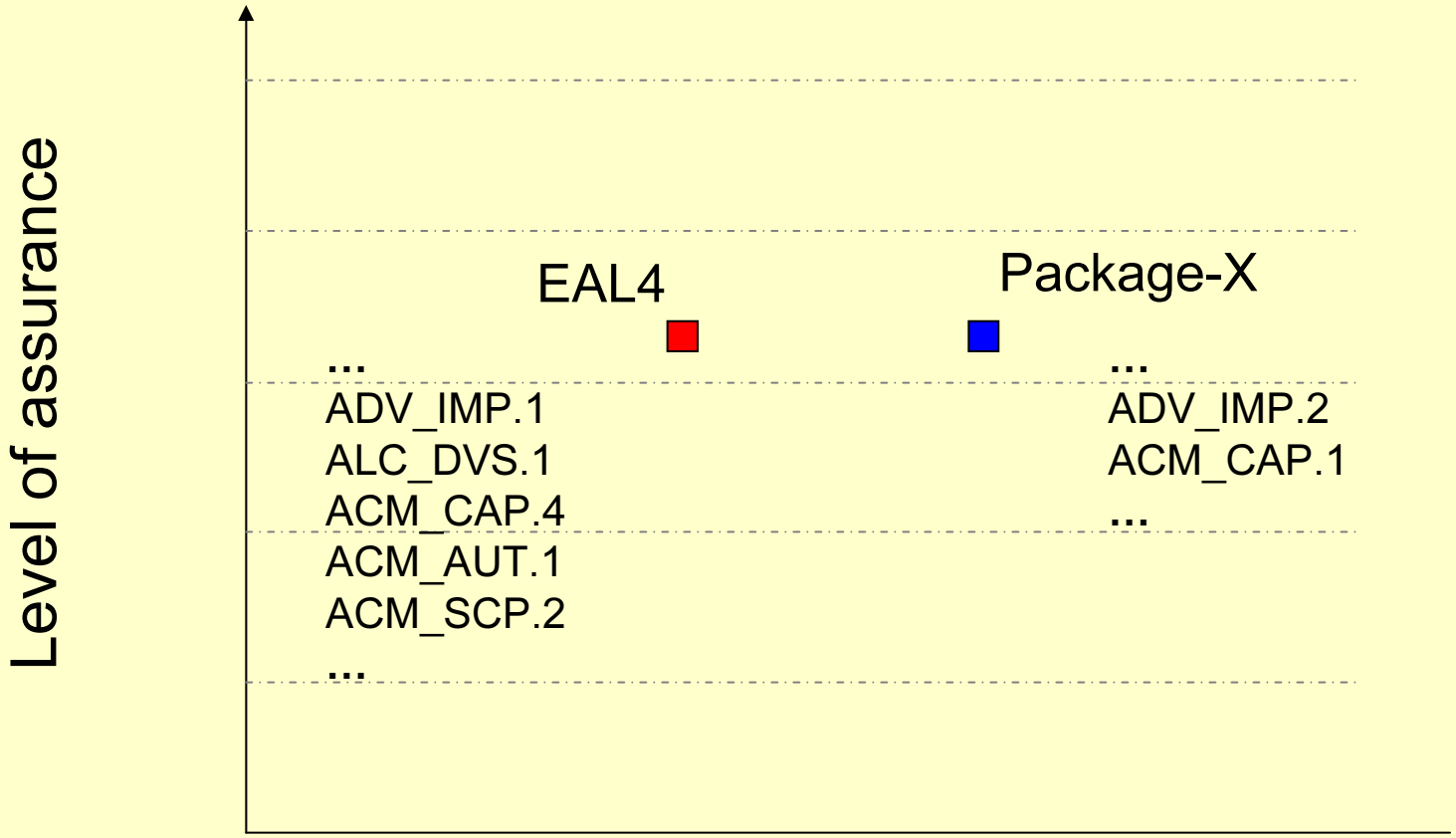
Common Criteria

Composition Stumbling Blocks

- What can be done if design evidence is not available?
  - Only evaluate composition at EAL1
  - Take a different approach to assurance… ACO
    - Focused on composition of components certified up to EAL4
    - Does not preclude composition of components above EAL4, but not specifically addressed

Common Criteria

Assurance philosophy



Common Criteria

Risk mitigation

- Have assurance in individual components
- Identify the portions of products not included in component evaluation
- Perform evaluation activities to mitigate risks that these additional portions contain weaknesses

Common Criteria

Composed TOE approach

- Understand how the components interact
  - Reliance of dependent component on base component
- Determine what has previously been evaluated
  - TSFI of base component
- Gain confidence in the “gaps”
  - Mainly rely on testing, use design information available
- When evaluate a composed TOE
  - When both components are certified
  - When the base component has been certified, in parallel to the dependent component evaluation

Common Criteria

Composed TOE approach

- Security Target (ASE)
- Reliance analysis (ACO_REL)
- Analysis of assurance measures applied to base component (ACO_COR)
- Details of interfaces and internals (ACO_DEV)
- Guidance for composed TOE (AGD)
- Testing of base component as used on composed TOE (ACO_TBT)
- Vulnerability analysis of composed TOE (ACO_VUL)

Common Criteria

Why new class

- Many similarities to component TOE evaluation, but significant differences
- Included additional methodology where possible (e.g. ASE, AGD), which is clearly identified to apply only when evaluating a composed TOE
- New requirements necessary to perform the various impact analyses

Common Criteria

Composition Assurance Packages

- The only way of achieving <EAL2> is by applying the requirements in the <EAL2> assurance package.
- There are many different ways of achieving a "level of confidence"
- CAPs provide given levels of confidence for composed TOEs
- EALs provide given levels of confidence for component TOEs

CAP<a> ≠ EAL<2>

Common Criteria

Composition Assurance Packages

- CAP<b> applied to two EAL<3> TOEs will result in a CAP<b> certificate

- However, CAP has been developed to be levelled along the same lines as EALs.
- CAP does not need to be applied to EAL1 TOEs to be composed, as a “traditional” EAL1 evaluation can still be performed.

Common Criteria

How does this relate to systems

- Approach to add components
  - Need to investigate whether addition of components is iterative or can add more than 2 components at once
- Only deals with technology side of systems
  - Not operational or environmental aspects